SECTION I—CLAIMS

Amendment to the Claims:

This listing of the claims will replace all prior versions and listings of claims in the application. No claims are amended. Claims 1-45 are, or remain canceled herein without prejudice. New claims 46-59 are added. Claims 46-59 remain pending in the application.

Listing of Claims:

1-45. (Canceled).

46. (New). A method of autodiscovery of an authenticator and packet forwarding device for network login, the method comprising:

receiving a connection request from an unauthorized user device at the packet forwarding device, the unauthorized user device requesting access to a network interfaced to the packet forwarding device;

blocking all packets received from the unauthorized user device at the packet forwarding device from accessing the network;

intercepting and redirecting a network login page of a user request to access the network by an authenticator discovery controller and returning the packet forwarding device's IP address;

assigning a temporary layer-3 address or a static layer-2 address to the unauthorized user device to gain access to the authenticator discovery controller, the network login controller, and user interface on the packet-forwarding device;

proceeding with the network login authentication and authorization using the network login

controller upon receiving the packet forwarding device's IP address from the authenticator discovery controller and using the temporary layer-3 address or the static layer-2 address assigned to the user device;

accessing the network login controller user interface and entering a user identification data;

determining whether the user identification data is authentic by the authentication server;

if the user has been denied permission to access the network by the authentication server;

the network login controller blocks the port to which the user is connected and leaves the port in an unauthorized state and the packet forwarding device in a non-forwarding mode;

if the user has been granted permission to access the network by the authentication server:

the network login controller unblocks the port to which the user connected by placing the port of the packet forwarding device into an authorized state and assigning the port to a permanent VLAN, and

replaces the temporary layer-3 address assigned to the user device with a permanent layer-3 address; and

resetting the port back into an unauthorized state and blocking the port, wherein the resetting is performed when at least one of the following occurs:

when a user successfully logs off the packet forwarding device,

when a connection from the user to the port is disconnected,

when no activity from the user occurs on the port for a duration of time, and

when an administrator forces the port to change its state.

47. (New) The method of claim 46, wherein intercepting and redirecting the network login page comprises: intercepting the user request to access the network and redirecting to a web

page comprising the network login page.

48. (New) The method of claim 46, wherein the user has been granted permission to access the network by the authentication server comprises the authentication server authenticating the user based on at least a user name and a password received from the unauthorized computing device.

49. (New) The method of claim 46, wherein accessing the network login controller user interface and entering the user identification data comprises the authenticator directing the unauthorized computing device to a Uniform Resource Locator (URL) address through which to access the user interface at a network login page.

50. (New) The method of claim 46, wherein determining whether the user identification data is authentic by the authentication server comprises:

sending the user identification data to the authentication server; and

receiving an indication from the authentication server that the user identification data is authentic and that the user associated with the user identification data is authorized to access the network.

51. (New) The method of claim 50, wherein sending the user identification data to the authentication server comprises:

creating a packet comprising the user identification data in accordance with a Remote Authentication Dial-In User Service (RADIUS) communications protocol; and

forwarding the packet to a RADIUS server for authentication.

52. (New) The method of claim 46, wherein the authenticator and packet forwarding device comprises a network switching device located at an edge of the network to provide packet-forwarding services into the network.

53. (New) A computer-readable storage medium having instructions stored thereon that, when executed by a processor in an authenticator and packet forwarding device, the instructions cause the processor to perform an autodiscovery method comprising:

receiving a connection request from an unauthorized user device at the packet forwarding device, the unauthorized user device requesting access to a network interfaced to the packet forwarding device;

blocking all packets received from the unauthorized user device at the packet forwarding device from accessing the network;

intercepting and redirecting a network login page of a user request to access the network by an authenticator discovery controller and returning the packet forwarding device's IP address;

assigning a temporary layer-3 address or a static layer-2 address to the unauthorized user device to gain access to the authenticator discovery controller, the network login controller, and user interface on the packet-forwarding device;

proceeding with the network login authentication and authorization using the network login controller upon receiving the packet forwarding device's IP address from the authenticator discovery controller and using the temporary layer-3 address or the static layer-2 address assigned to the user device;

accessing the network login controller user interface and entering a user identification data;

determining whether the user identification data is authentic by the authentication server;

if the user has been denied permission to access the network by the authentication server;

the network login controller blocks the port to which the user is connected and leaves the port in an unauthorized state and the packet forwarding device in a non-

forwarding mode;

if the user has been granted permission to access the network by the authentication server:

the network login controller unblocks the port to which the user connected by placing the port of the packet forwarding device into an authorized state and assigning the port to a permanent VLAN, and

replaces the temporary layer-3 address assigned to the user device with a permanent layer-3 address; and

resetting the port back into an unauthorized state and blocking the port, wherein the resetting is performed when at least one of the following occurs:

when a user successfully logs off the packet forwarding device,

when a connection from the user to the port is disconnected,

when no activity from the user occurs on the port for a duration of time, and

when an administrator forces the port to change its state.

54. (New) The computer-readable storage medium of claim 53, wherein intercepting and redirecting the network login page comprises: intercepting the user request to access the network and redirecting to a web page comprising the network login page.

55. (New) The computer-readable storage medium of claim 53, wherein the user has been granted permission to access the network by the authentication server comprises the authentication server authenticating the user based on at least a user name and a password received from the unauthorized computing device.

56. (New) The computer-readable storage medium of claim 53, wherein accessing the network login controller user interface and entering the user identification data comprises the authenticator directing the unauthorized computing device to a Uniform Resource

Locator (URL) address through which to access the user interface at a network login page.

57. (New) The computer-readable storage medium of claim 53, wherein determining whether the user identification data is authentic by the authentication server comprises:

sending the user identification data to the authentication server; and

receiving an indication from the authentication server that the user identification data is authentic and that the user associated with the user identification data is authorized to access the network.

58. (New) The computer-readable storage medium of claim 57, wherein sending the user identification data to the authentication server comprises:

creating a packet comprising the user identification data in accordance with a Remote Authentication Dial-In User Service (RADIUS) communications protocol; and

forwarding the packet to a RADIUS server for authentication.

59. (New) The computer-readable storage medium of claim 53, wherein the authenticator and packet forwarding device comprises a network switching device located at an edge of the network to provide packet-forwarding services into the network.